INTERNET DOCUMENT INFORMATION FORM

A. :Report Title: Information Dominance for the Warfighter: The Present to Year 2025

B. DATE Report Downloaded From the Internet _18 Mar 98

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): The Under Secretary of Defense for Acquisition and Technology

D. Currently Applicable Classification Level: Unclassified

E The foregoing information was compiled and provided by:
DTIC-OCA, Initials:___PM_________**Preparation Date:**18 Mar 98

DIST- A

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

"Information Dominance for the Warfighter:

The Present to Year 2025"

Keynote Address of

The Under Secretary of Defense for Acquisition and Technology

Honorable Paul C. Kaminski

to the

AFCEA InfoTech 1996 Conference

Dayton, OH

October 8, 1996

Good morning. I had such a great time last year—I could not resist the invitation to this year's 1996 InfoTech conference. A great deal has changed in the past year. It reminds me of the words probably spoken by Eve when she and Adam left the Garden of Eden: "Adam," said Eve, "We live in a time of great transition."

We live in a similar time today. We have won a great Cold War with the former Soviet Union—but five years later, we still have not found a term better than "post-Cold War" to describe the current era. It is a term that describes where we are today relative to the past. But what about our relationship with the future?

Our society, and indeed, those of the first and third world nations alike, are riding the wave of the "Information Revolution." It is driven by the breathtaking advances being made in microprocessors and telecommunications. The general trend we have seen since the 1970s has been about a ten-thousand fold improvement in processing capability at nearly the same cost.

The advances are proceeding at a rate described by Moore's Law. This empirical relationship says that computer chips get twice as powerful every 18 months. The same $2500 that bought the original Macintosh in 1984 with 128K of random access memory (RAM) and the Motorola 68000 processor now buys a 180 MHz Performa with a RISC-based PowerPC processor, 32MB of RAM, 1.2GB hard drive, an eight-speed CD-ROM, and a 28.8k Fax Modem. We project that we will have another thousand fold improvement over the next 15 years at the rate of advance predicted by Moore's Law.

This kind of progress is transforming the world we live in. Last month, we celebrated the 50th anniversary of the first modern digital computer. It was known as the Electronic Numerical Integrator and Computer, or ENIAC for short. ENIAC was developed by the University of Pennsylvania and installed at the Army's Ballistic Research Laboratory, in Aberdeen, Maryland. It had been designed to help solve a pressing Cold War defense issue of the late 1940s—calculating the trajectories of artillery rounds. This anniversary coincided with the award of a new DoD contract to install, at that same location, high-speed supercomputers with a computational capacity in excess of 100 million times that of the original ENIAC.

Where I live in Fairfax County, Northern Virginia, parents of students in the gifted-talented program are expected to have a 486 or better home computer with internet e-mail accounts. Twelve year old students—7th graders—have the e-mail addresses of their teachers and regularly send homework over the internet. Many of these students have access to free e-mail services. And when they are not e-mailing their homework to teachers, they are engaging in old fashioned "chit-chat" with their friends and relatives across the country via the internet.

Some of these twelve year olds will be America's warfighters in the early 21st century. They along with America's coalition partners, will help define and secure that elusive "post-Cold War" future I spoke of earlier. To operate successfully on the 21st Century battlefield our warfighters will need a superior awareness of the battlefield. It means knowing the status of enemy and friendly forces. It even means having intelligence on enemy intentions. Our forces will need this to make decisions faster than their adversaries. This is what it means to have "information dominance."

INFORMATION DOMINANCE

To achieve information dominance, I see a greater move to what I call large scale "system-of-systems" architectures with global span and highly networked, mobile elements. It will place a premium on being able to put together complex software and the various legacy components that we have developed in the way of sensor systems, communication systems and weapon systems.

There is a great range of opportunity for improvements here without major investments in the component systems themselves, by providing the systems engineering and the system integration glue to tie together in a better way those components. Many of you sitting in the audience today are playing a critical role in these endeavors, understanding as you do, the aspects of many of these systems and how they can be better configured and tied together to be more effective in a closed cycle sense.

The implications of system-of-systems architectures are enormous. It means that any particular system depends on a wide variety of separate physical and software support elements and any particular element is supporting a wide variety of different systems. We are taking existing distributed systems of this sort and building larger systems out of them.

Earlier last summer, for example, the submarine and special operations community just completed a related, very successful Advanced Concept Technology Demonstration—ACTD—to integrate attack submarines into the nation's larger system-of-systems C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) architecture. In this case, a nuclear attack submarine, the USS CHICAGO, took control of the Predator Unmanned Aerial Vehicle in a demonstration with Navy SEALs off San Clemente Island, California.

This effort is a significant first: it is the first example of a Predator vehicle and sensors being controlled from a Navy submarine. Some people in the submarine community have commented that "this is the most exciting thing that has happened in submarine warfare since the nuclear reactor." I agree with them—rather than having a 15 foot periscope, the submarine effectively had a 15,000 foot periscope.

For the purposes of this demonstration, the submarine was configured with a super high frequency 23 dB gain flat plate antenna, similar to that used for direct broadcast TV, except adapted for seagoing conditions unique to submarines. A SUN SPARC workstation was used for directional control of the antenna. A JDISS terminal was put on-board to insure a video re-broadcast at 32 kilobits-per-second.

The Predator was directed to conduct target surveillance in order to plan a real-time SEAL insertion-including dynamic re-tasking and bomb damage assessment. The demonstration included control of the UAV from the submerged attack submarine at periscope depth from a range of about 100 nautical miles.

A number of new systems are coming on-line in addition to unmanned aerial vehicles like the Predator. We are developing and fielding systems like JSTARS, or the Joint Surveillance Target Attack Radar System. From the outside, JSTARS looks like an ordinary Boeing 707—one you might expect to find in some commercial air cargo fleets. But inside, as many of you know, the jet is packed with an advanced moving target indicator and synthetic aperture radar and advanced computer processing and communications systems.

The jet is the airborne platform for a powerful surveillance, targeting and battle management "system-of-systems" capability—one well suited to the requirements of the NATO Alliance Ground Surveillance system. We've used this capability to great advantage in Bosnia. For example, JSTARS has flown 51 missions in Bosnia, covering a total area of 747 million square kilometers or about 75 times the land area of the United States. On a typical mission, JSTARS spent an average of eight and half hours on station; and filling up the 60 Gbytes of mass storage on-board. Over the 51 missions, 6,950 radar service requests were met. There were 38 million total detections and 26,000 total revisits. To secure an overwhelming advantage, commanders will need a third capability: the C3 and planning tools to achieve something I call "Dominant Battle Cycle Time" or the ability to act before an adversary can react.

Our strategy is to ensure that US forces possess an overwhelming capability of "information dominance." Just as the United States possessed an overwhelming nuclear capability and extended a "nuclear umbrella" over our allies during the cold War, so too will the United States extend an "information umbrella" over our coalition partners in the 21st Century.

This is being demonstrated in Bosnia today. The NATO IFOR is breaking new ground on how we view interoperability with our friends and allies. Even before IFOR, our Warsaw initiative was aimed at improving interoperability of command and control systems with the nations of central Europe. IFOR demonstrated that this need was real.

Fundamentally, our command, control, communications, intelligence and logistics systems must be interoperable. Generally, we are achieving this in IFOR through setting common standards, as well as providing access to a secure tactical internet with multi-level security through our Info-Comm initiative.

In the future, information dominance will allow the US to deploy small, more lethal, and dispersed units to accomplish missions performed today by much larger forces. We are examining such new warfare concepts in ACTDs such as SEA DRAGON. The key to the effectiveness of these small units will be the possession of superior dynamic situational awareness and communications. Offensively, these small units will be able to concentrate direct and remote fires on a massed enemy force. Defensively, they will enjoy the advantage of being dispersed. Small unit operations is just one of the new emerging warfighting concepts enabled by information dominance.

INFORMATION SYSTEMS SURVIVABILITY

Our information dominance strategy has a down side a well. Our ability to project power will become increasingly dependent on the power of our computing systems and their integrity and robustness over time. DoD systems and networks are interconnected with a large number of other large-scale systems such as public phone systems, the power grid, our banking systems, and our air traffic control systems. Each of these systems is itself a large-scale distributed computing and networking system, and all of them are based on readily available computing technology with their own large-scale vulnerabilities.

It is in this context that I would like to talk to you about "Information System Survivability." when I use this term, I mean the ability of large-scale systems-of-systems to continue adequate performance of critical services even after attacks have taken place—physical attacks on the networks, logic attacks on the computing elements, or internal compromises.

This is a different focus than the traditional security focus, where security people tend to focus on keeping the bad guys out by building a barrier or fire wall. The focus here is to do as much of that

as you possibly can, but it acknowledges the fact that no barrier can be perfect. At some point, building higher walls simply leads to diminishing returns—a Maginot Line. Therefore the critical question is what do you do when the barrier is penetrated.

The goal of an effective information survivability strategy is to maintain a smooth, tight, and effective decision cycle that runs within the cycle of our adversaries even though enemies can possibly intrude into your systems and you have absorbed information warfare attacks. We still must be able to act and react quicker than our adversaries can in this environment.

As we move to large-scale systems-of-systems, one has to acknowledge that as you do this, you integrate the vulnerabilities of the different components. And so a failing or compromised router can have implications, not just for a single system, but for a variety of component systems and for the overall system-of-systems. A compromised piece of software in any of these nodes might be able to reach across and destroy other systems' components running within that same node.

To design survivability into our information systems, it is my sense that we will have to look beyond building higher—and more costly—barriers to entry. Barriers have a role, but we need a broader view. One such view involves looking at how living organisms, and perhaps populations and societies operate. So it is worthwhile to ask: What is it about these things that lets them be survivable? If you look at organisms, they almost all have some barrier to entry, skin, membranes and the like, things to keep out attacking elements.

This barrier in living organisms is an "immune system." So that even after the bad guys got in, we have ways of finding them and getting them out. Many living organisms have sacrificial organisms, like tonsils—no one really knows why tonsils exist in the human body, but one thing they do right now is they get infected and, having got infected, they let the body's immune system see the infecting elements. So they are an information-gathering element that lets the rest of the system respond.

We see enormous degrees of fault tolerance and the ability to maintain homeostasis in organisms, that is, to preserve the critical functions, say by restricting blood flow to the extremity to maintain heat in the interior. Now, interestingly enough, you see exactly these same kinds of functions going on at the macro scale in societies. We have public health systems at every level. We have market economies that allocate resources—a macro scale version of homeostasis of the body. We have duplication of skills across individuals, so that no individual is indispensable and we see the organization into subgroups that autonomously attack goals without central coordination or without a lot of it. And finally, at the population level we see that variability within the species is key to the survival of the species.

Now, you might ask why in the world am I talking about all of this, what does this have to do with keeping our information system secure? The answer is that these are very suggestive of ways we might think of engineering a strategy for survivable systems-of-systems.

At least three major elements are suggested by these biological and social models. The first is that the survivable system of systems has to have a public health infrastructure, something that can protect the population by noticing the attack, responding to that attack, trying to understand larger plans of the attack, having means for isolating and quarantining it and for gathering information and understanding it. The public health systems at the macro level depend upon the immune system at the micro level.

Second, it needs to be adaptive as it loses resources, either because those resources are diverted to deflecting attacks or because resources are compromised. It needs to reallocate its resources to get its critical task done.

Now, the final major theme is that of diversity. We know from looking at biological systems that if you plant all of the Midwest m the same variety of corn, sooner or later an insect or disease is going to show up and you're going to lose all of it. It's not only that you'll lose all of it.

Diversity is an important property of populations—for large-scale systems it's a key to their survival. It's not only that, but it's a hedge against the unknown. You can't possibly foresee every attack, but by having enough diversity you can make sure that most attacks don't succeed in taking out everything and therefore that you have enough resources left to reconstitute.

The problem for our computer ecology, as it were, is that economic forces make us move in exactly the opposite direction. There is, after all, a reason why 90% of the systems on desktops are more or less the same system and while 90% of our servers are more or less the same system—Windows in one case, UNIX in the other, at the moment. Over time, what those systems are will change, but the general forces towards uniformity are very strong and powerful.

The challenge then is to figure out ways to get variability even though there are large-scale forces forcing us towards uniformity. You can imagine that general approach of looking for variability within common interfaces as a compromise between the economic forces and robust survivability. We can have uniformity at the interfaces, but variability within. We are very much looking for techniques that give us different ways for engendering that variability at different levels of the computing hierarchy.

At the moment there does not exist a community organized around these immature intellectual ideas. You don't look at computer science departments for example and see groups in them labeled survivability or adaptive large-scale systems or anything like that. Within the DoD, the DARPA Information Technology Office is pursuing a focused program of applied research along these lines. At the national level, the Presidential Commission on Critical Infrastructures is addressing some of the larger policy issues associated with implementation of a national "information survivability" strategy.

I think it's a given that when you start a new field like this, it's going to be disorganized for awhile. We will have lots of competing ideas fighting against one another and no clear way of deciding between them. I think that will be characteristic of this field for awhile. It is a critical new field—one with new terms like "canary," "honeypot," and "tarbaby." We will need to attract the best and brightest to this new career field. For our combat forces, information dominance is too powerful to pass up because of potential vulnerabilities—we must address these issues head on.

DUAL-USE SYNERGY

One final note is in order at this point. "Information survivability" is not just a DoD issue. There is a substantial amount of overlap in the interests of the DoD, banks, telephone companies and public utilities in implementing survivable information systems. In some cases, the private sector vulnerability is a more urgent and challenging concern. The desire of banks to protect electronic funds-transfer systems comes to mind immediately. This alignment of public and private interests implies that there is great potential to leverage investments through cooperative development of dual-use technologies.

SUMMARY

In summary, it is clear that we encounter some difficult challenges as well as some significant opportunities as we enter the next century. Our combat forces will increasingly exploit our "information dominance" to turn inside an adversary's decision cycle. System-of-systems architectures will provide this kind of information superiority and will dominate the 21st century battlefield. In this environment, the United States will need to extend an "information umbrella" over our friends and allies during coalition operations.

Reliance on large system-of-systems architectures will expose our forces to significant vulnerabilities. The traditional approach, providing a wall around our systems, will not be fully effective against information warfare attacks. Our systems must be robust and continue adequate performance of critical services even after attacks have taken place.

To design survivability into our information systems, it is my sense that perhaps we will have to take a broader view and perhaps benefit from understanding how living organisms, populations and societies survive.

Information survivability or defensive information warfare is not just a DoD issue. It is a national issue. It is a concern of both public and private institutions. My sense is that there is a tremendous opportunity to leverage investment through cooperative development of dual use technologies.

In a famous 1837 lecture, Ralph Waldo Emerson asked his audience, "If there is any period one would desire to be born in, is it not the age of revolution, when the old and new stand side by side...?" Like Emerson, we, too, live in age of revolution—the continuing explosion of information systems raises rich new possibilities as well as some important new vulnerabilities.

Our challenge is to exploit the possibilities and eliminate the vulnerabilities. In this way, we too will live in a period one would desire to be born in. I look forward to working with you as we proceed to equip and sustain US forces in the years ahead.

Thank you all.